Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

In the Matter of *Call Authentication Trust Anchor*	WC Docket No. 17-97

COMMENTS OF TRANSACTION NETWORK SERVICES

August 14, 2017

Paul Florack
TRANSACTION NETWORK SERVICES
11480 Commerce Park Drive
Reston, VA 20191

TABLE OF CONTENTS

Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

In the Matter of *Call Authentication Trust Anchor*	WC Docket No. 17-97

COMMENTS OF TRANSACTION NETWORK SERVICES

I. INTRODUCTION AND SUMMARY

Transaction Network Services ("TNS") hereby submits the following comments in response to the Federal Communication Commission's ("FCC" or "Commission") *Call Authentication Trust Anchor Notice of Inquiry* regarding ATIS/SIP Forum proposals thus far, as well as the Commission's governance role and other public policy considerations of the proposals. TNS fully supports the Commission's efforts to protect consumers from fraudulent and harassing robocalls.

TNS thanks the FCC for the opportunity to comment on (1) the "governance proposal in Phase 2", (2) the "technical operation and implementation of the SHAKEN/STIR proposal" and (3) the "scope of the proposals as to Signaling System 7 (SS7) and international calling as well as other public policy considerations.

II. BACKGROUND

TNS' Telecommunication Services Division addresses the full needs of over 400 wireless and wireline operators in the US and globally. Its portfolio of network signaling, roaming and

clearing, wireless fraud management, and database and registry solutions enables the successful delivery of subscriber services anywhere at any time.

From small rural operators in the US to the largest multi-national telecommunication providers around the globe, our portfolio of mobile network, identity, discovery and routing solutions enables the successful and reliable delivery of subscriber solutions around the globe, while our clearing, settlement and anti-fraud solutions enables the successful delivery of subscriber services anywhere at any time.

With the launch of TNS Call Guardian ("Call Guardian"), whose customers include Sprint and Verizon Wireless through Cequint, the company's wholly-owned subsidiary that delivers enhanced caller identification and call management services to wireless operators, TNS provides a lightweight and flexible solution to identify and filter unwanted robocalls, via real-time telephone number reputation analysis. Call Guardian is available for both TDM/SS7 and VoIP, supporting several access protocols, and offers our partners the most accurate and timely detection of robocallers in the market through real-time analysis of over 1 billion call events per day. TNS' comments below address TNS Call Guardian with respect to its role as the Analytics Server included in IETF and FCC readouts.

TNS operates one of the largest North American SS7 networks, handling hundreds of millions of SS7 call routing and lookup events per day. As a result, TNS has significant visibility into the continued importance and usage of the SS7 protocol for routing telephone calls. Additionally, a significant portion of nuisance, fraudulent, and illegal robocalling is targeted at landline/traditional end users. Lastly, the large number of years remaining in the migration away from SS7 continues to confound the most conservative estimates. Given this backdrop, TNS believes that solutions to this problem space for non-SIP signaling frameworks are important and

worthwhile, and believes that the commission should foster and support these initiatives. Two specific classes of solutions that have complementary merit in the non-SIP and multi-protocol solution space are (1) the Analytics Server, and (2) solutions such as the IETF's emerging "Out of Band STIR". These solutions have the notable advantage of being less impactful on the signaling infrastructure and standards, far less complex, and the potential for a wider near-term adoption in multi-protocol communication environments. These solutions avoid the fundamental character of "In-Band STIR", the addition of data elements that must be embedded and retained within the SIP messages as they traverse what are often multiple networks from originator to terminator. TNS will continue to contribute to specification and implementation of solutions to the problem space targeted at SS7 and mixed protocol signaling, as well as the SIP environment.

III. DISCUSSION

A. The Commission Must Examine the STIR/SHAKEN Landscape.

TNS applauds the Commission's continued efforts to address malicious and harassing robocalls. Alongside a Do-Not-Originate list and the blocking of calls from unallocated and unassigned numbers as outlined in the Commission's previous NPRM, CG Docket No. 17-59, STIR/SHAKEN adoption will address a segment of the robocall problem.[1] The proposed process of authentication and verification of callers is predicated on technology and methodology used elsewhere with trust and security.

TNS' comments seek to guide discussion about the extent to which open roles, policy, costs, and other business questions have been examined, and the extent to which they remain to be addressed. TNS also seeks to determine whether the Commission has similarly evaluated and

[1] *Advanced Methods to Target and Eliminate Unlawful Robocalls*, CG Docket No. 17-59, Notice of Proposed Rulemaking and Notice of Inquiry, 32 FCC Rcd 2306, 2331-34 (statements of Chairman Pai and Commissioner Clyburn) (rel. Mar. 23, 2017) (*2017 Call Blocking NPRM and NOI*).

promoted other in-market robocall protection solutions. Per industry analysis and discussion, there is no silver bullet that addresses the robocall problem in totality.[2]

1. Certificate Management and Governance– Phase 2.

Regarding Section III B of the NOI, TNS submits that selection of governance authorities, policy administrators, and certificate authorities should be open to competitive bid with one of the criteria being that any such provider be neutral and not in the business of providing other services related to the STIR/SHAKEN framework..

2. Costs.

TNS supports investigation of the costs of implementing call authentication, and suggests that this question may need to receive higher priority, given the necessity of smaller providers' participation in order to ensure that both authentication and verification are able to take place. STIR/SHAKEN appears to depend on end-to-end functionality, which places particular emphasis on the study of feasibility for small providers, wholesalers, and international gateways to be able to participate.

In Section D, para. 46 of the NOI, the Commission has inquired about the high-level costs associated with implementation of STIR/SHAKEN. TNS would suggest that a more in-depth analysis is likely required in order to ensure that guidance is not provided that cannot be borne by calling providers.

3. Risks.

The Commission must consider that authenticating origination as a tactic runs the risk of pressing bad actors to increase their use of legitimate numbers, where the callers' intent cannot

[2] Alliance for Telecomm. Indus. Solutions, *Developing Calling Party Spoofing Mitigation Techniques: ATIS' Role* 2 (2016), http://www.atis.org/01_resources/whitepapers/ATIS_Robocalling_Summary.pdf.

be addressed without an Analytics Server.[3] The Analytics Server role has been discussed in previous industry documentation, but has not been addressed or evaluated to-date by the FCC.

The Analytics Server, a service which is available today, must be evaluated in the current landscape, in which implementation of STIR/SHAKEN will require considerable time and an indeterminate cost, and will not necessarily address calls coming from international gateways, from which a significant number of robocalls originate. In addition, today, the Analytics Server is able to evaluate calls traversing both SIP and SS7 networks. The Commission must consider the complementary, necessary, and ongoing role played by the Analytics Server, which examines and communicates intent.

4. Penalties and Incentives.

The Commission must consider whether there are repercussions for not taking part in a solution that is heavily dependent on end-to-end participation. TNS' guidance is that there cannot be penalties in an environment where the costs remain undetermined, and no method of cost recovery has been authorized.

Additionally, the FCC must evaluate whether guidance will include repercussions for allowing bad calls through, or for being unable to verify good calls.

5. Authorizations and Assertions.

Per the issue raised in Background para. 4 of the NOI, TNS urges the FCC to promote further examination around how legitimate spoofers are authorized. These use cases exist and must be addressed in a thorough evaluation prior to implementation.

[3] Alliance for Telecomm. Indus. Solutions, *Mitigation Techniques for Unwanted Robocalls: Updates on ATIS and Other Key Industry Initiatives* (2016), https://www.atis.org/01_news_events/webinar-pptslides/robocallslides_final.pdf.

Subscribers must be vetted. What mechanism will permit this and how is that burden borne by calling providers?

Additionally, further clarity around whether STIR/SHAKEN's assertion of Identity is over the calling provider, the telephone number making the call, or the subscriber would be helpful.

6. Tracebacks.

The FCC must consider how post-call reporting will work. Consumers must be educated about the availability of tracebacks. To which entity does this fall? Tracebacks are valuable components of STIR/SHAKEN. How will tracebacks be addressed and by whom?

TNS is not so much invested in the conclusion as the requirement that policy around these many open questions be considered prior to guidance that providers embrace the methodology and move ahead.

7. Good Samaritan Exemption.

In para. 16, the NOI solicits comments on the nature of existing laws and regulations as possible barriers to adoption. It would be helpful to the industry for the FCC to provide an opinion as to whether or not the Good Samaritan exemption of 47 U.S.C. § 230 "PROTECTION FOR PRIVATE BLOCKING AND SCREENING OF OFFENSIVE MATERIAL" immunizes providers of an interactive computer service (e.g. a mobile app) that delivers a registered user a technical means to control their private blocking and screening of communications that they or their service provider believe to be fraudulent, unlawful, harassing, or otherwise objectionable (i.e. illegal and unwanted robocalls) from civil liability.

8. International Calls.

As para. 40 of the NOI acknowledges, the problem of nuisance, fraudulent, and illegal robocalling is not one that respects geopolitical boundaries. Bad actors may, in fact, benefit from geopolitical boundaries, if the solutions put in place are limited by those boundaries. Certainly the STIR specification has no inherent technical limitation that results from SIP signaling that may traverse geopolitical boundaries. Furthermore, the SHAKEN profile accompanying the STIR standard may serve as a template for adoption, internationally. That stated, each geopolitical authority must engage in the time-consuming process of evaluation and adoption. For this reason, the Analytics Server component, which is less intrusive and time consuming to adopt, requires active Commission consideration.

IV. CONCLUSION

TNS supports STIR/SHAKEN and is in alignment with the FCC's goals regarding robocalls. Per the FCC's question in Discussion para. 14 regarding promotion of adoption of STIR/SHAKEN, timing, feasibility, business questions, roles, and costs largely remain unknowns. TNS has pointed to specific areas in this response which require further discussion before the FCC moves to policy around adoption and timelines.

Further, TNS asks the FCC to evaluate the recommendation for an Analytics Server, advocated by both the IETF and the FCC's October 26, 2016 *Robocall Strike Force Report,* in a similar manner.[4] Given that all are in agreement about the urgency of a solution to the robocall problem, it is germane that current in-market solutions address many of its aspects, and relieve current pressures around feasibility, cost, and timing. Data analytics-based solutions are (1)

[4] Federal Communications Commission, *Robocall Strike Force Report* (2016), p.12, https://transition.fcc.gov/cgb/Robocall-Strike-Force-Final-Report.pdf.

already under deployment by some major carriers, (2) may be more naturally adaptive to the changing techniques of nuisance callers, (3) may be more applicable to a larger set of practices employed by the bad actors, (4) are far less impactful on the signaling infrastructure and signaling standards, (5) are less complex to adopt, and (6) can be deployed in a timely manner and not dependent on deployment of an all-IP network .

Of particular importance is the fact that the Analytics Server is agnostic regarding call origination and network path. Internationally-originating, wholesale, VoIP, and TDM/SS7 callers are evaluated by the Analytics Server. However, some of the in-market solutions introduce concerns. For this reason, this essential concurrent piece of the robocall solution would benefit from similar discussion.

For further review, TNS has shared its thoughts on the holistic approach that includes Do-Not-Originate, STIR/SHAKEN, and the Analytics Server role in this white paper https://www.tnsi.com/forms/robocall-white-paper/.